FlexEdge Secure SD-WAN

7.1

How to install Forcepoint FlexEdge Secure SD-WAN in FIPS mode

Revision A

Contents

Introduction

You can use the Forcepoint FlexEdge Secure SD-WAN in FIPS mode to comply with Federal Information Processing Standards (FIPS).

The Forcepoint FlexEdge Secure SD-WAN solution includes Secure SD-WAN Engines, Forcepoint FlexEdge Secure SD-WAN Manager (SMC) server components, and SMC user interface components. The basic SMC components are the Management Server, Log Server, and one or more Management Clients. The Management Client is the user interface for the SMC. You use the Management Client for all configuration and monitoring tasks.

There are two main ways to deploy the SMC:

- You can use a Secure SD-WAN Manager appliance that ships with a Management Server and a Log Server pre-installed on it.
  You can also install the SMC Appliance as a virtual machine on virtualization platforms such as VMware ESX. For more information, see *Installing SMC Appliance software on a virtualization platform* in the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.
- You can install the SMC components on Windows or Linux platforms.

In a FIPS environment, you must use Secure SD-WAN Engines that run on purpose-built Secure SD-WAN Engine appliances.

Product name change

This release introduces change to product and component names. For more information about the change to product and component names, refer to the **About this Help** section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Important

1) Some documentations, knowledge base articles, and other support information are still using the old product name.

2) There is no change in the Engine local user interface.

3) The IPS role has transitioned now from L2FW mode to L3FW mode.

Deprecated features

The following features are no longer supported:

- SSL VPN Portal.
- Web Portal User Interface is deprecated and is not available by default.

For more information on deprecated features, refer to the **About this release** section in the *FlexEdge Secure SD-WAN Manager 7.1.0 Release Notes*.

Installing the SMC Appliance in FIPS mode

To use the SMC Appliance in a FIPS environment, you must install the SMC Appliance in FIPS mode.

You must complete the following main steps:

1) Enable FIPS mode on the SMC Appliance.

2) Check the SMC Appliance self-tests.

3) Install the Management Client.

Related tasks

Enable FIPS mode on the SMC Appliance on page 3
Check the SMC Appliance self-tests on page 5
Install the Management Client on page 13

Enable FIPS mode on the SMC Appliance

You must enable FIPS mode when you install the SMC Appliance.

Steps

1) Turn on the SMC Appliance.

2) Accept the EULA.

3) Select **Begin**, then press **Enter**.

4) Select the keyboard layout for accessing the SMC Appliance on the command line.

5) Enter the administrator account name and password.

> **Note**
>
> The administrator account and password are used for command line access to the SMC Appliance and for access to the Management Client. The administrator account is created with unrestricted permissions (superuser).

   a) Enter the account name.

      This field is case sensitive and limited to eight characters.

   b) Enter the password.

      The password is case sensitive. The password must be at least ten characters long and contain at least one number.

   c) Enter the password again.

6) (Optional) Configure a bootloader password.

   If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the SMC Appliance.

   a) Press the space bar to configure a bootloader password.

   b) Enter the password.

   c) Enter the password again.

7) Make your security selections.

   a) Select FIPS mode.

   b) Select 256-bit encryption as the security strength.

8) To enable network interface configuration, select **Disabled**, then press **Enter**.

9) Complete the network interface configuration for the primary network interface for management.

   a) Select **Enable interface**.

   b) Select **Primary**.

   c) Complete the network configuration fields for the interface.

10) (Optional) Complete the network interface configuration for the secondary network interface for management.

   a) Select **Enable interface**.

   b) Select **Secondary**.

c) Complete the network configuration fields for the interface.

11) Enter a host name for the Management Server.

12) (Optional) Enter one or more IPv4 or IPv6 addresses in the DNS server fields.

> **Note**
>
> CIDR notation is not allowed.

13) (Optional) If you do not want to use NTP, disable it in the NTP settings.

14) Select the time zone.

15) Set the date and time.
You are prompted to review the configuration.

16) Select **Confirm**, then press **Enter**.

Result

When the installation is complete, the SMC Appliance restarts.

Check the SMC Appliance self-tests

The SMC Appliance contains several modules that run self-tests when the SMC Appliance starts.

Known answer tests (KAT) and pairwise consistency tests (PCT) are run for the software cryptographic modules.

Integrity check verifies the ECDSA signature of a catalog file of the SHA-256 hashes of all binaries.

Noise source health tests include a Repetition Count Test and a Chi-Squared test to fulfill the role of the Adaptive Proportion Test as specified by NIST SP 800-90B.

Bouncy Castle FIPS Java API software module self-tests

Algorithm	Type
Software integrity	HMAC-SHA-256
AES	KAT
CCM	KAT
AES-CMAC	KAT
FFC KAS	KAT
DRBG	KAT, Continuous, Health Checks
DSA	KAT, PCT
ECDSA	KAT, PCT
GCM/GMAC	KAT
HMAC	KAT

Algorithm	Type
ECC KAS	KAT
SP 800-108 KBKDF	KAT
RSA	KAT, PCT
SHS	KAT
TDES	KAT
TDES-CMAC	KAT
Extendable-Output functions (XOF)	KAT
Key Wrapping Using RSA	KAT
Key Transport Using RSA	KAT
NDRNG	Continuous
DH	PCT
ECDH/ECCDH	PCT

OpenSSL FIPS self-tests

Algorithm	Type
Software integrity	HMAC-SHA-256
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
AES XTS	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT
DSA	KAT, PCT
ECDSA	KAT, PCT
DRBG	KAT, Continuous
Diffie-Hellman	KAT
EC Diffie-Hellman	KAT
SHA1	KAT
SHA2	KAT
SHA3	KAT
KBKDF	KAT
PBKDF2	KAT

NSS Cryptographic Module self-tests

Algorithm	Type
AES	KAT
TDES	KAT
DSA	KAT
ECDSA	KAT
RSA	KAT
SHS	KAT
HMAC	KAT
DRBG	KAT
Software integrity	DSA signature verification

Check the self-test results in the console. The self-test messages are also sent to the SMC Appliance syslog.

- If the Bouncy Castle FIPS Java API cryptographic module self-test fails, the server application fails to start, and an error message is shown on the console and the appliance halts its execution automatically.

  ```
  fipssmc: ERROR: FIPS SMC Bouncy Castle
  fipssmc: FIPS System Shutdown
  ```

- If a power-up self-test fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

  ```
  fipstest:Performing FIPS NSS crypto selftests...
  Fatal FIPS Error: fipstest:ERROR:FIPS NSS crypto selftest failed: /lib/fips/fipstest-ossl: 255
  ```

  ```
  fipstest: Performing FIPS OpenSSL crypto selftests…
  Fatal FIPS Error: fipstest:ERROR:FIPS OpenSSL crypto selftest failed: /lib/fips/fipstest-ossl: 1
  ```

- If the file system integrity check fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

  ```
  fipscheck: Performing FIPS integrity check…
  Fatal FIPS Error: fipscheck:ERROR:FIPS integrity check failed. /usr/bin/smca-fipscheck: 255
  ```

- If a noise source health test fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

  ```
  fipsrngdtest: Performing FIPS rngd self test...
  Fatal FIPS Error: fipsrngdtest:ERROR:FIPS rngd self test failed: 1
  ```

Next steps

- If the self-tests succeed, continue configuring the SMC Appliance.
- If a self-test fails, restart the SMC Appliance manually. It does not restart automatically.
- If a self-test continues to fail, reset the SMC Appliance to factory settings. See section *Reset the SMC Appliance to factory settings*.

Related tasks

Install the Management Client on page 13

Reset the SMC Appliance to factory settings

If a self-test fails on the SMC Appliance, reset the SMC Appliance to factory settings.

Steps

1) Connect to the SMC Appliance command line using one of these options.
   - Connect a keyboard to a USB port and a monitor to the VGA port, then press **Enter**.
   - Connect to the IP address of the iDRAC port, then start the virtual console on the **Server Properties** tab.
2) Turn on the SMC Appliance, then at the boot menu, select **VCDROM**.
3) Select **Manual Installation** and **Begin**.
4) Select **Fresh Install**, then press **Enter**.
5) (Optional) Highlight **Securely wipe drive**, then press the space bar.
6) Select **Next**, then press **Enter**.
   You are prompted to review the configuration.
7) Select **Confirm**, then press **Enter**.
8) Install the SMC Appliance in FIPS Compatible Mode.

Installing the SMC in FIPS mode

If you do not have a pre-installed SMC Appliance, you must enable FIPS restrictions on the Management Server, the Log Server, and the Management Client when you install them.

For detailed installation instructions and information about hardware requirements for third-party hardware, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide* and the *Forcepoint FlexEdge Secure SD-WAN Release Notes*.

CAUTION

In Linux, cryptographic modules use /dev/random as the source of randomness. Using /dev/random as the source of randomness can block installation, startup, or even execution. We recommend that you install and run an entropy daemon, such as jitterentropy-rngd or haveged.

You must complete the following main steps:

1) Download the SMC software from https://support.forcepoint.com, then check the file integrity.
2) Obtain licenses for all the SMC servers and the Secure SD-WAN Engine in the License Center at https://stonesoftlicenses.forcepoint.com.
   Generate the licenses based on your Management Server proof-of-license (POL) code.
3) Install the Management Server, the Log Server, and the Management Client.

Enable FIPS restrictions during the installation.

4) Start the Management Client.

5) Install the licenses for the Management Server and Log Server.

Start the installation

Start the Installation Wizard on the computer where you want to install the SMC components.

Steps

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.
   Decompress the .zip file.
   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

3) Select the language for the installation, then click **OK**.
   The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

   Tip

   Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) (Optional) Select where to install the SMC, then click **Next**.
   The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

   Note

   If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.

8) Select where to create shortcuts, then click **Next**.
   These shortcuts can be used to manually start components and to run some maintenance tasks.

9) Select **Typical** as the installation type, then click **Next**.

Install the Management Server

Continue the installation in the Installation Wizard to configure the options for the Management Server.

Steps

1) Configure the settings, then click **Next**.

Option	Description
Select Management Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Advanced Management Server Options	When selected, you can configure additional options on another page. Select this option if you want to: ▪ Disable the use of 256-bit encryption for communication between the Management Server and the Secure SD-WAN Engines. ▪ Enable the use of SMC Web Access to run the Management Client in a web browser. ▪ (Linux only) Enable integrating NSX-V with Secure SD-WAN.
Install as an Additional Management Server for High Availability	When selected, you can configure additional options on another page.
Enable FIPS Configuration Restrictions	You must enable this option to use the SMC in FIPS mode.
Install the Management Server as a Service	When selected, the server starts automatically.

2) If you selected **Advanced Management Server Options** on the previous page, select the features to enable, then click **Next**.

Option	Description
Enable and Configure SMC Web Access	When enabled, administrators can access the SMC in a web browser. You can run the Management Client in a web browser instead of installing the Management Client locally. On Linux platforms, xvfb-run must be installed under `/usr/bin`. You can specify another path in the Management Server properties after the installation has completed.
Enable OWASP encoding	When enabled, the SMC API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks when you use the SMC API in a web browser. **Note** When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.
Enable NSX Service (Linux only)	When enabled, allows integrating NSX-V with Secure SD-WAN.
256-bit Security Strength	When enabled, 256-bit encryption is used for communication between the Management Server and the Secure SD-WAN Engines. This option is selected by default.

3) If you enabled SMC Web Access, configure the settings, then click **Next**.

Option	Description
Port Number	Enter the TCP port number that the service listens to. By default, port 8085 is used when SMC Web Access is enabled on the Management Server and port 8083 when enabled on the Web Portal Server. **Note** Make sure that the listening port is not in use on the server.
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.
Certificate Distinguished Name	Administrators must use an HTTPS connection to access and use the Management Client. Enter the distinguished name in LDAP string format for the certificate used to secure the HTTPS connection. Example: `dn=smc,dc=demo,dc=com`
Certificate Algorithm	Select the algorithm and key length for the certificate used to secure the HTTPS connection.
Certificate Signer	Select the signer for the certificate used to secure the HTTPS connection. You can use the Internal Certificate Authority or the certificate can be self-signed.

4) Enter a user name and password to create a superuser account, then click **Next**.

Important

This is the only account that an administrator can use to log on after the installation has been completed.

Install the Log Server

Continue the installation in the Installation Wizard to configure the options for the Log Server.

Steps

1) Configure the settings, then click **Next**.

Option	Description
Select Log Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
IP Address(es) of the Management Server(s) that will control this Log Server	Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
Certify the Log Server during the installation	When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server.
Port on which the Log Server will receive data	Enter the port number that the server receives data on.
Enable FIPS Configuration Restrictions	You must enable this option to use the SMC in FIPS mode.
Install the Log Server as a Service	When selected, the server starts automatically.

2) (Optional) Click **Choose** to browse to a different storage folder for log data.

> **Note**
>
> Remote locations are not suitable for active storage, as quick and reliable access is required.

3) Click **Next**.

Finish the installation

Review the configuration options that you set in the Installation Wizard, then finish the installation.

Before you begin

If you are installing any server components as a service on a Windows system, make sure that the Services window is closed before you proceed.

Important

This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.

Steps

1) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

   Depending on the options, you selected, you might be prompted to generate certificates during the installation.

   When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

2) When the installation has completed, click **Done**.

   Note

   If any Log Server or Web Portal Server certificate was not retrieved during the installation, retrieve a certificate manually before starting the server.

Install the Management Client

If you did not install the Management Client on the same computer as the Management Server or if you are using the SMC Appliance, you must separately install the Management Client in FIPS mode on each administrator's computer.

For system requirements, see the SMC release notes for your version.

As an alternative to installing the Management Client, you can use SMC Web Access. You can enable these features when installing the Management Server, or you can enable them later.

Steps

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.

   Decompress the .zip file.

   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

3) Select the language for the installation, then click **OK**.

   The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

   Tip

   Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) (Optional) Select where to install the SMC, then click **Next**.

   The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

   Note

   If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.

8) Select where to create shortcuts, then click **Next**.

   These shortcuts can be used to manually start components and to run some maintenance tasks.

9) Select **Management Client Only** as the installation type, then click **Next**.

10) When prompted to select the cryptographic algorithms, select **Restricted Cryptographic Algorithms Compatible with FIPS**.

11) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

    Important

    This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.

12) When the installation has completed, click **Done**.

Start the Management Client

After you have started the Management Server, start the Management Client.

Steps

1) If you installed the Management Client locally on the workstation, do the following:
   - (Windows) Use the shortcut icon or run the script `<installation directory>/bin/sgClient.bat`.
   - (Linux) Run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed.

2) If you enabled SMC Web Access to run the Management Client in a web browser, do the following:
   a) In a web browser, browse to the URL of the server that you configured the SMC Web Access feature on.

      The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.

      Example where SMC Web Access is enabled on the default port 8085 on the Management Server: `https://127.0.0.1:8085`

   b) Enter your user name and password, then click **Log On**.

Installing the Secure SD-WAN Engine in FIPS mode

To use the Secure SD-WAN Engine in a FIPS environment, you must install the Secure SD-WAN Engine in FIPS mode.

In a FIPS environment, you must use Secure SD-WAN Engines that run on purpose-built Secure SD-WAN Engine appliances.

You must complete the following main steps:

1) Create an element for the Secure SD-WAN Engine in the Management Client.

2) Enable FIPS mode in the properties of the Secure SD-WAN Engine element.

3) Install the Secure SD-WAN Engine in FIPS mode.

4) Check the results of the self-tests on the Secure SD-WAN Engine appliance.

Create an element for the Secure SD-WAN Engine

Use the Management Client to create the Secure SD-WAN Engine element.

These steps are the high-level tasks. For more information, see the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Steps

❓ For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, create an Secure SD-WAN Engine, then define the properties in the Engine Editor.

   Follow the normal process to define the properties of an Secure SD-WAN Engine, with these exceptions:

   - On the **Advanced Settings** branch, select **FIPS-Compatible Operating Mode**.
   - On the **Advanced Settings** > **Log Handling** branch, select a suitable setting for the **Log Spooling Policy** option, depending on your network environment.

2) Save the initial configuration.

   Note

   Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

Install the Secure SD-WAN Engine in FIPS mode

Use the Secure SD-WAN Configuration Wizard to install the Secure SD-WAN Engine in FIPS mode.

These steps are the high-level tasks. For complete installation instructions, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*. Before upgrading, read the *Forcepoint FlexEdge Secure SD-WAN Release Notes* for the version you are upgrading to.

Note

Secure SD-WAN Engine appliances come with Secure SD-WAN Engine software pre-installed. Before setting the Secure SD-WAN Engine to use FIPS mode, upgrade the Secure SD-WAN Engine software to the version that you want to use.

Steps

1) Download the Secure SD-WAN Engine software from https://support.forcepoint.com/Downloads, then validate the checksums.

   > **Note**
   >
   > Save the Secure SD-WAN Engine upgrade .zip file to the root directory of the USB drive or DVD media.

   For information about obtaining the installation files, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.

2) Upgrade the Secure SD-WAN Engine software to the version that you want to use.
   a) In the Secure SD-WAN Configuration Wizard, select **Firewall/VPN** as the role.

   b) Select **Upgrade**.

   c) In the **Select Source Media** dialog box, select the appropriate media type, then click **OK**.
      The software update signature is verified.

   d) Click **OK**.
      The upgrade starts.

   e) Select **Set kernel in FIPS mode after reboot**.

   f) Click **OK**.

   Secure SD-WAN appliance restarts and displays the upgraded version.

3) Configure the Secure SD-WAN Engine with the Secure SD-WAN Configuration Wizard.
   Follow the normal process to define the Secure SD-WAN Engine properties, with these exceptions:
   - Select **FIPS-Compatible Operating Mode**.
     This option enables the FIPS 140-2 cryptographic module.
   - (Optional) To use the cryptographic module updated for FIPS 140-3, select **FIPS 140-3 Compatible Mode**.

4) To verify FIPS-Approved mode of operation, verify that the following messages are shown on the console when the Secure SD-WAN Engine appliance restarts:

   ```
   FIPS: rootfs integrity check OK
   ```

   This message confirms that the module's integrity test has been executed successfully.

   ```
   FIPS power-up tests succeeded
   ```

   This message confirms that the FIPS power-up self-tests have been executed successfully. If the power-up tests fail, a power-up test error message is shown and the module restarts.

Check the Secure SD-WAN Engine self-tests

The Secure SD-WAN Engine contains the OpenSSL FIPS, SafeZone FIPS Cryptographic Module, Secure SD-WAN Cryptographic Library, and Secure SD-WAN Cryptographic Kernel Module. The modules run several self-tests when the Secure SD-WAN appliance starts.

The modules perform these tests:

- Cryptographic algorithm known answer tests (KAT)
- Software integrity tests using HMAC or digital signature verification
- Conditional self-tests for CTR-DRBG
- Pair-wise consistency test (PCT) on generated RSA, DSA, and ECDSA keys
- File system integrity check that verifies the ECDSA signature of the whole partition containing all binaries
- Noise source health tests include a Repetition Count Test and a Chi-Squared test to fulfill the role of the Adaptive Proportion Test as specified by NIST SP 800-90B.

OpenSSL FIPS self-tests

Algorithm	Type
Software integrity	HMAC-SHA-256
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
AES XTS	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT
DSA	KAT, PCT
ECDSA	KAT, PCT
DRBG	KAT, Continuous
Diffie-Hellman	KAT
EC Diffie-Hellman	KAT
SHA1	KAT
SHA2	KAT
SHA3	KAT
KBKDF	KAT
PBKDF2	KAT

Secure SD-WAN Cryptographic Kernel Module self-tests

Algorithm	Algorithm
Software Integrity	HMAC-SHA-256

Algorithm	Algorithm
AES	KAT
TDES	KAT
HMAC	KAT
SHA	KAT

SafeZone FIPS Cryptographic Module self-tests

Algorithm	Algorithm
Software integrity	ECDSA signature verification
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
AES XTS	KAT
AES CMAC	KAT
TDES	KAT
RSA	KAT, PCT
DSA	KAT, PCT
ECDSA	KAT, PCT
DRBG	KAT, Continuous
SHS	KAT
SHA-3	KAT
KBKDF	KAT

Check the self-test results in the console.

- If a cryptographic self-test or a noise source health test fails, an error message is shown on the console and the appliance is restarted automatically. Noise source health tests are automatically executed as part of the self-tests when OpenSSL and SafeZone are loaded.

  ```
  FIPS: OpenSSL self-tests FAILED, rebooting…
  Cryptographic Kernel Module self tests failed
  FIPS: Cryptographic module self-tests FAILED, rebooting...
  ```

  ```
  FIPS: rootfs integrity check FAILED, rebooting…
  ```

Next steps

- If the self-tests succeed, continue configuring the Secure SD-WAN Engine.
- If the problem persists, reset the Secure SD-WAN appliance to factory settings. See section *Reset the Secure SD-WAN appliance to factory settings*.

Reset the Secure SD-WAN Engine appliance to factory settings

If a cryptographic self-test or the file system integrity check fails, you must reset the appliance to factory settings.

If the appliance is otherwise functioning correctly, but you want to destroy all cryptographic keys on the Secure SD-WAN Engine appliance, you can also reset the appliance to factory settings from the Management Client. For more information, see the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Steps

1) Restart the Secure SD-WAN Engine appliance, then select **System restore options** from the boot menu.

2) Select **Advanced data removal options**.

3) Select the number of overwrite passes.

   A larger number of overwrites is more secure, but it might take a considerable amount of time depending on the appliance storage capacity.

   - For one pass, select **1 pass overwrite**.
   - For multiple passes, select **Custom**, then enter the number of overwrite passes.

4) Install the Secure SD-WAN Engine in FIPS mode.

© 2024 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 18 January 2024